TRIBUNAL SUPERIOR DO TRABALHO
PRESIDÊNCIA

ATO N. 183/GDGSET.GP, DE 27 DE MAIO DE 2019 (*)

Estabelece as diretrizes de segurança da informação no âmbito do Tribunal Superior do Trabalho.

O PRESIDENTE DO TRIBUNAL SUPERIOR DO TRABALHO, no uso de suas atribuições legais e regimentais, considerando a Lei de Acesso à Informação, Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto no inc. XXXIII do art. 5º, no inc. II do § 3º do art. 37 e no § 2º do art. 216 da Constituição da República e dá outras providências

considerando a Lei Geral de Proteção de Dados, Lei nº 13.709, de 14 de agosto de 2018, que dispõe sobre a proteção de dados pessoais

considerando o Ato TST.GP. nº 255/2013, que disciplina a composição e as atribuições do Comitê Gestor de Segurança da Informação do Tribunal Superior do Trabalho – CGSI

considerando o Ato Conjunto TST.CSJT nº 27/2013, que define os papéis e as responsabilidades da unidade gestora, do gestor de sistema, da unidade de negócio e do usuário de sistemas informatizados e de bases de dados no âmbito do Tribunal Superior do Trabalho e do Conselho Superior da Justiça do Trabalho

considerando a Norma Complementar nº 14/IN01/DSIC/GSIPR, e sua Revisão 1, que estabelece princípios, diretrizes e responsabilidades relacionados à Segurança da Informação (SI) para o tratamento da informação em ambiente de Computação em Nuvem e em órgãos e entidades da Administração Pública Federal (APF), direta e indireta

considerando o conjunto de normas ABNT NBR ISO/IEC 27000, que especificam os requisitos para estabelecer, implementar, manter e melhorar continuamente o sistema de gestão da segurança da informação

considerando as melhores práticas para a proteção e para o controle da informação referenciadas nas disciplinas do COBIT e nos processos da biblioteca ITIL

considerando a necessidade de ampliar as diretrizes e os padrões de segurança, a fim de garantir um ambiente tecnológico controlado e seguro, de forma a oferecer as informações necessárias aos processos de trabalho deste Tribunal com integridade, confidencialidade e disponibilidade

Fonte: Boletim Interno [do] Tribunal Superior do Trabalho, Brasília, DF, n. 45, p. 9-22, 13 nov. 2020. Republicação 1.

considerando a necessidade de regulamentar o acesso à rede de computadores, aos sistemas informatizados, aos bancos de dados, à internet, à intranet, à rede sem fio, às redes sociais, ao teletrabalho e ao VPN (Virtual Private Network – Rede Privada Virtual)

considerando a necessidade de regulamentar o uso do serviço de correio eletrônico corporativo, da estrutura de diretórios na rede de computadores, de programas e aplicativos, de equipamentos de tecnologia da informação, da utilização de serviços em nuvem

considerando a necessidade de regulamentar as práticas de mesa limpa e tela limpa, de gestão de riscos, de continuidade e de vulnerabilidades do ambiente tecnológico; bem como o controle, monitoramento e a auditoria de recursos tecnológicos no âmbito do Tribunal

considerando os danos potenciais decorrentes de acessos a sítios e aplicativos indevidos ou inadequados na internet, da instalação de programas não homologados e inadequados, bem como o risco de contaminação de programas maliciosos nas estações de trabalho e nos dispositivos móveis,

RESOLVE:

Art. 1º Definir a Política de Segurança da Informação do Tribunal Superior do Trabalho, cabendo aos usuários a observância de suas disposições e às unidades administrativas, no âmbito de suas competências, a implementação e o acompanhamento de ações para a segurança da informação.

Art. 2º Para efeitos deste ato aplicam-se as seguintes definições:

I – Ambiente tecnológico: conjunto de recursos que utiliza ou disponibiliza serviços de tecnologia da informação e sistemas de informação do Tribunal;

II – Ativos de informação: base de dados e arquivos, contratos e acordos, documentação de sistema, informações sobre pesquisa, manuais de usuário, material de treinamento, procedimentos de suporte ou operação, planos de continuidade do negócio, procedimentos de recuperação, trilhas de auditoria e informações armazenadas, aplicativos, sistemas, ferramentas de desenvolvimento e utilitários, equipamentos computacionais, equipamentos de comunicação, mídias removíveis e outros equipamentos;

III – Central de Serviços de TI: equipe dedicada a determinadas atividades de suporte técnico dos serviços de TI, a quem cabe promover o contato inicial entre os usuários e a Secretaria de Tecnologia da Informação e Comunicação – SETIN;

IV – Confidencialidade: princípio de segurança da informação que garante o acesso à informação somente a usuários autorizados;

V – Conteúdo evasivo: arquivo ou programa com artifícios capazes de burlar os mecanismos de segurança da informação estabelecidos no TST, permitindo a saída de informações ou dados;

VI – Conteúdo intrusivo: arquivo ou programa com artifícios capazes de burlar os mecanismos de segurança da informação estabelecidos no TST, permitindo a entrada de informações ou dados;

VII – Controle de acesso: conjunto de recursos que efetivam as autorizações e as restrições de acesso aos ativos de informação;

VIII – Correio eletrônico corporativo ou correio corporativo: são consideradas corporativas as caixas de correio eletrônico dos usuários internos e colaboradores constantes da solução de e-mail gerenciada pelo TST;

IX – Disponibilidade: princípio de segurança da informação que garante aos usuários autorizados acesso à informação e aos ativos correspondentes;

X – Integridade: princípio de segurança da informação que salvaguarda a exatidão e a completeza da informação e dos métodos de processamento;

XI – Licença de uso: cessão de direito de utilização do programa de computador, outorgada pelo detentor dos direitos autorais e da propriedade intelectual, por prazo determinado ou indeterminado, mediante pagamento único ou periódico;

XII – Programa de computador: conjunto de instruções em linguagem natural ou codificada executado por computador, dispositivos, instrumentos ou equipamentos periféricos, com base em técnica digital ou analógica, para fazê-los funcionar de modo e para fins determinados;

XIII – Programa de livre distribuição: programa que oferece período de avaliação gratuito, após o qual é requerido pagamento pela licença de uso ou que pode ser utilizado gratuitamente por tempo indeterminado;

XIV – Programa de terceiro: programa que não foi elaborado pela equipe de informática da SETIN;

XV – Programa malicioso: programa criado para causar algum dano ao computador infectado, seja apagando dados, capturando informações ou alterando o funcionamento normal da máquina;

CAPÍTULO I
DO CONTROLE DE ACESSO À REDE DE COMPUTADORES

Art. 3º Os serviços de acesso à rede de computadores do Tribunal abrangem: estrutura de diretórios de rede, intranet, internet, correio eletrônico e rede sem fio.

§ 1º O acesso padrão à rede de computadores do Tribunal é assim regulado:

I – Para usuário interno: é permitido o acesso a toda rede de computadores do Tribunal;

I – Para usuário previdenciário: é permitido o acesso à intranet;

III – Para usuário colaborador: é permitido o acesso à rede de computadores do Tribunal e à internet, bem como o envio e recebimento de mensagens eletrônicas;

IV – Para usuário externo: é permitido o acesso à rede sem fio do Tribunal, em situações devidamente autorizadas.

§ 2º Em casos de comprovada necessidade de serviço, o responsável pela unidade poderá solicitar à SETIN, por meio da Central de Serviços de TI, motivadamente, autorização para acesso à internet ou para envio e recebimento de mensagens externas de correio eletrônico a usuários colaboradores, bem como acesso à internet a usuários externos.

Art. 4º A solicitação de concessão de acesso à rede de computadores do Tribunal será feita pelo responsável da unidade à SETIN, por meio da Central de Serviços de TI.

§ 1º Na solicitação de acesso à rede de computadores do Tribunal para usuários internos, deve conter nome completo e código do usuário interessado, bem como os serviços solicitados, conforme descritos no art. 3º.

§ 2º No caso de usuários colaboradores ou externos, a solicitação conterá, ainda, o tempo de validade do acesso à rede de computadores do Tribunal, sendo o limite máximo a duração do estágio, do contrato ou da permanência.

§ 3º A Seção de Gestão da Segurança da Informação – SGSI poderá, constatado o não cumprimento deste Ato, a qualquer momento, solicitar a suspensão do acesso concedido ao usuário.

§ 4º É vedada a utilização de perfil de administrador local ou de administrador de domínio para pessoal que não seja técnico da SETIN.

Art. 5º O acesso à rede de computadores do Tribunal e seus serviços dar-se-á pela combinação nome de usuário e senha, que é pessoal e intransferível.

§1º A senha deverá ter um tamanho mínimo de 8 (oito) caracteres alfanuméricos, contendo pelo menos 3 (três) dos seguintes tipos de caracteres: um número, uma letra maiúscula, uma letra minúscula ou um caractere especial, devendo ser evitada aquela de fácil dedução. (Redação alterada pelo art. 1° do ATO TST.GP. N° 437, de 10/11/2020.) **(Redação alterada pelo art. 1° do ATO TST.GP. N° 437, de 10/11/2020.)**

§2º A senha de acesso à rede de computadores do Tribunal será alterada a cada 6 (seis) meses. **(Redação alterada pelo art. 1° do ATO TST.GP. N° 437, de 10/11/2020.)**

§ 3º O sistema impedirá o usuário de reutilizar as suas 3 (três) últimas senhas.

Art. 6º É proibido aos usuários ceder sua senha para o acesso de terceiros à rede de computadores do Tribunal.

Art. 7º A solicitação de revogação de acesso à rede de computadores do Tribunal será feita pelo responsável da unidade à SETIN, por meio da Central de Serviços de TI, quando houver o desligamento do usuário de sua unidade.

Art. 8º O acesso à rede de computadores do Tribunal será monitorado e registrado pela SETIN, podendo a qualquer momento ser efetuada auditoria, conforme o Capítulo XIV deste Ato.

CAPÍTULO II
DO CONTROLE DE ACESSO AOS SISTEMAS INFORMATIZADOS E AOS BANCOS DE DADOS

Art. 9º A solicitação de concessão de acesso aos sistemas informatizados do Tribunal será encaminhada à SETIN, por meio da Central de Serviços de TI, pelo responsável da unidade ao gestor do respectivo sistema.

§ 1º Na solicitação de acesso aos sistemas informatizados do Tribunal, deverá constar o nome completo e o código do usuário interessado, bem como o tipo de acesso a ser concedido e com a sua justificativa.

§ 2º No caso de usuários colaboradores ou externos, a solicitação deverá conter ainda o tempo de validade do acesso aos sistemas informatizados do Tribunal, sendo o limite a duração do estágio, do contrato ou da permanência.

Art. 10. O acesso aos sistemas informatizados e aos bancos de dados será monitorado e registrado pela SETIN, podendo a qualquer momento ser efetuada auditoria, conforme estabelecido no Capítulo XIV deste Ato.

Art. 11. A revogação de acesso aos sistemas informatizados do Tribunal será feita pelo gestor da unidade no sistema de permissionamento (PS) quando houver o desligamento do usuário de sua unidade.

Art. 12. Os servidores responsáveis pelo desenvolvimento de sistemas do TST, da ENAMAT e do Conselho Superior da Justiça do Trabalho – CSJT, quando esses tiverem hospedados na infraestrutura tecnológica do TST, poderão ter acesso aos sistemas em produção e aos bancos de dados para realizar manutenções, mediante autorização expressa do gestor do sistema.

Art. 13. O gestor do sistema poderá, justificadamente, solicitar a suspensão ou o cancelamento do acesso do usuário ao sistema informatizado do Tribunal.

CAPÍTULO III
DO CONTROLE DE ACESSO À INTERNET E À INTRANET

Art. 14. A concessão de acesso à internet e à intranet no âmbito do Tribunal seguirá o previsto no Capítulo I deste Ato.

Art. 15. O uso não apropriado do acesso à internet e à intranet será passível de apuração de responsabilidade.

Parágrafo único. Entende-se por uso não apropriado o acesso a sítios ou quaisquer outros serviços:

I – de conteúdo considerado ofensivo, ilegal ou impróprio;

II – que apresentem vulnerabilidade de segurança ou possam comprometer a integridade e a disponibilidade da rede de computadores do Tribunal;

III – que possuem conteúdos evasivos e/ou intrusivos.

Art. 16. A comprovação, por auditoria, do uso não apropriado implicará o bloqueio imediato da internet para o usuário e a comunicação ao responsável da unidade de lotação do usuário.

Art. 17. Caberá à SGSI, a qualquer momento, o bloqueio de sítios cujo conteúdo seja considerado não apropriado.

Art. 18. É vedada a transferência (download e upload) de arquivos:

I – relacionados à pornografia;

II – de quaisquer formatos de áudio ou vídeo;

III – executáveis;

IV – com conteúdo prejudicial à segurança do ambiente tecnológico desta Corte.

§ 1° No caso do inciso II, a transferência poderá ser autorizada mediante justificativa:

I – encaminhada à SETIN por magistrado ou gestor detentor de cargo em comissão;

II – contendo expressamente a relação entre a atividade desempenhada e a demanda.

§ 2° O acesso aos serviços de streaming de vídeo, como o YouTube, é franqueado somente às contas governamentais do respectivo serviço ou rede social, mediante controle de banda a ser determinado pela CITEC, considerando os recursos tecnológicos disponíveis.

Art. 19. O acesso à intranet poderá ser efetuado a partir de computadores que estejam fora das dependências do Tribunal mediante a combinação nome de usuário e senha da rede de computadores do TST.

Art. 20. A CITEC é a unidade responsável pelo controle de banda na internet e pelo seu monitoramento.

Parágrafo único. Caso necessário, serão estabelecidos limites e quotas para a transferência de dados dos usuários, objetivando garantir a disponibilidade de banda para os serviços ofertados pelo TST à sociedade.

Art. 21. O acesso à internet ou à intranet, partindo de computadores situados no âmbito do Tribunal, será monitorado e registrado pela SETIN, podendo a qualquer momento ser efetuada auditoria, conforme estabelecido no Capítulo XIV deste Ato.

CAPÍTULO IV
DO CONTROLE DE ACESSO À REDE SEM FIO

Art. 22. A rede sem fio dará acesso à internet, sendo vedada a comunicação direta com a rede interna do Tribunal.

Art. 23. Os usuários internos deste Tribunal terão acesso à rede sem fio.

Art. 24 A solicitação de concessão de acesso à rede sem fio do Tribunal para usuários colaboradores e externos será feita pelo responsável da unidade, utilizando a Central de Serviços de TI.

§ 1° O responsável da unidade assinará o Termo de Responsabilidade, disponibilizado na intranet.

§ 2° O acesso dos usuários externos será revogado em 180 dias, caso o Termo de Responsabilidade não indique data e justificativa para sua manutenção além deste período.

I – Os acessos que durarem mais do que 180 (cento e oitenta) dias deverão observar a política de senhas definida no Capítulo I.

§ 3° A conta de usuários externos deverá ser bloqueada e a senha trocada ao final do serviço prestado ou do evento realizado.

Art. 25. O acesso à rede sem fio será realizado mediante a combinação nome de usuário e senha da rede de computadores do Tribunal.

Art. 26. O acesso efetuado pela rede sem fio do Tribunal deverá atender ao disposto nos capítulos de I a III deste Ato e será monitorado e registrado pela SETIN, podendo a qualquer momento ser efetuada auditoria, conforme estabelecido no Capítulo XIV deste Ato.

Art. 27. A solicitação de revogação de acesso à rede sem fio do Tribunal será realizada pelo usuário à SETIN, por meio da Central de Serviços de TI.

CAPÍTULO V
DO CONTROLE DE ACESSO A REDES SOCIAIS

Art. 28. O acesso a redes sociais está sujeito à necessidade para o trabalho mediante justificativa motivada.

§ 1º A solicitação de acesso a redes sociais deverá ser encaminhada à SETIN, por meio da Central de Serviços de TI, por Ministros, Chefes de Gabinete, Gestores detentores de cargo em comissão CJ4 responsável.

§ 2º A justificativa, integrante do Termo de Responsabilidade, deverá conter expressamente a relação entre a atividade desempenhada e a demanda e será analisada pela unidade de Segurança da Informação em relação ao nível de exposição às ameaças computacionais.

§ 3º Para a SECOM e para a CDEP, a solicitação poderá ser feita respectivamente pelo Secretário ou pelo Coordenador.

CAPÍTULO VI
DO CONTROLE DE ACESSO AO TELETRABALHO E À VPN

Art. 29. A solicitação de concessão de acesso remoto, para execução do teletrabalho, será formalizada pelo responsável da unidade à SETIN, por meio da Central de Serviços de TI.

§ 1° No ambiente de teletrabalho, o usuário contará com o mesmo perfil de acesso que detém na rede de computadores e nos sistemas informatizados do Tribunal.

§ 2° A disponibilização de novas aplicações no ambiente de teletrabalho será realizada após a homologação da Coordenadoria de Suporte Técnico aos Usuários – CSUP.

Art. 30. A Coordenadoria de Infraestrutura Tecnológica CITE deverá disponibilizar ferramental para o teletrabalho que proporcione:

I – Segurança do meio de comunicação;

II – Autenticação dos usuários;

III – Limite de acesso restrito aos recursos computacionais segundo as necessidades de cada usuário.

Art. 31. É recomendável ao usuário em regime de teletrabalho:

I – Manter seu computador com as últimas atualizações e correções de segurança instaladas;

II – Utilizar somente sistema operacional e programas licenciados;

III – Manter programa antivírus atualizado;

IV – Habilitar o firewall do sistema operacional;

V – Não expor dados e informações sensíveis do TST a terceiros;

VI – Não salvar as senhas de acesso ao ambiente de teletrabalho nos navegadores ou outros programas;

VII – Alterar imediatamente suas senhas de rede e sistemas em caso de perda, roubo, descarte ou manutenção do equipamento utilizado para teletrabalho;

VIII – Configurar a rede sem fio doméstica com pelo menos o protocolo WPA2, alterando a senha padrão do roteador.

IX – Armazenar os documentos corporativos exclusivamente nos locais adequados providos no ambiente de teletrabalho;

X – Utilizar equipamento apropriado às atividades de trabalho remoto;

XI – Observar o disposto nos Capítulos XII e XIII.

Parágrafo único. O licenciamento do sistema operacional e demais programas instalados na estação de trabalho doméstica do usuário é de sua inteira responsabilidade.

Art. 32. A solicitação de revogação de acesso ao ambiente de teletrabalho será realizada pelo responsável da unidade à SETIN, por meio da Central de Serviços de TI.

Art. 33. O acesso realizado pelo ambiente de teletrabalho será monitorado e registrado pela SETIN, podendo a qualquer momento ser efetuada auditoria, conforme estabelecido no Capítulo XIV deste Ato.

Art. 34. Os artigos deste Capítulo valem para o acesso realizado por meio do mobilidade.tst.jus.br ou por VPN.

CAPÍTULO VII
DA UTILIZAÇÃO DO CORREIO ELETRÔNICO CORPORATIVO

Art. 35. Os serviços de correio eletrônico corporativo do Tribunal serão destinados ao desempenho das atividades funcionais dos usuários, sendo vedado o seu uso para assuntos particulares.

§ 1º Os serviços de correio eletrônico corporativo não serão disponibilizados para usuários previdenciários.

§ 2º O acesso aos serviços de correio eletrônico corporativo permanecerá disponível por um prazo de 30 (trinta) dias corridos a contar da publicação da aposentadoria.

Art. 36. A concessão de acesso ao correio eletrônico corporativo do Tribunal seguirá o previsto no Capítulo I deste Ato.

Art. 37. O uso não apropriado do correio eletrônico corporativo do Tribunal é passível de apuração de responsabilidade do usuário.

Parágrafo único. Por uso não apropriado, considera-se o envio de mensagens de correio eletrônico contendo:

I – materiais obscenos, ilegais ou antiéticos;

II – materiais preconceituosos ou discriminatórios;

III – materiais caluniosos ou difamatórios;

IV – propagandas com objetivos comerciais;

V – listas de endereços eletrônicos dos usuários do correio eletrônico corporativo do Tribunal;

VI – vírus ou qualquer outro programa malicioso;

VII – material de natureza político-partidária ou sindical, que promova a eleição de candidatos para cargos públicos eletivos, clubes, associações e sindicatos;

VIII – material protegido por leis de propriedade intelectual;

IX – entretenimentos;

X – assuntos ofensivos;

XI – arquivos de áudio, vídeo, imagem ou texto que não sejam de interesse específico do trabalho;

XII – SPAM.

Art. 38. O limite de tamanho das caixas postais corporativas do Tribunal será fixado em norma interna de responsabilidade da CITEC, disponível na intranet do Tribunal.

Art. 39. Os anexos das mensagens de correio eletrônico não poderão exceder o tamanho estabelecido em norma interna de responsabilidade da CITEC, disponível na intranet do Tribunal.

§ 1º É vedado ao usuário o envio de anexo que configure o uso não apropriado do correio eletrônico corporativo, conforme o art. 37.

§ 2º É vedado o envio ou recebimento de mensagem eletrônica com mais de 20 (vinte) arquivos anexados.

Art. 40. É responsabilidade do usuário do correio eletrônico corporativo do Tribunal:

I – utilizar o correio eletrônico para objetivos e funções inerentes às suas atribuições funcionais;

II – eliminar periodicamente as mensagens contidas nas caixas postais;

III – não permitir acesso de terceiros ao correio eletrônico por meio de sua senha.

Art. 41. O envio e o recebimento de mensagens do correio eletrônico corporativo do Tribunal serão registrados pela SETIN, podendo a qualquer momento ser efetuada auditoria, conforme estabelecido no Capítulo XIV deste Ato.

CAPÍTULO VIII
DA UTILIZAÇÃO DA ESTRUTURA DE DIRETÓRIOS NA REDE DE COMPUTADORES

Art. 42. A concessão de acesso à estrutura de diretórios da rede de computadores do Tribunal seguirá o previsto no Capítulo I deste Ato.

Art. 43. O usuário da rede de computadores do Tribunal terá acesso a um ou mais diretórios de rede referentes à unidade de sua lotação, mapeados em sua estação de trabalho com a denominação "K:", "G:", ou outro mapeamento que estiver disponível, com os direitos de leitura e escrita.

§ 1º Diretórios de rede são para uso compartilhado, não sendo permitida a criação de diretório de rede para uso pessoal.

§ 2º Os responsáveis pelas unidades serão os gestores de seus respectivos diretórios de rede, devendo responder por seu uso e definir as permissões de acesso dos usuários sob sua responsabilidade, podendo ainda encaminhar solicitação de criação de novas estruturas de diretórios na rede de computadores do Tribunal.

Art. 44. Os responsáveis pelas unidades poderão solicitar a criação de diretórios de rede para auxiliar em projetos ou atividades compartilhadas com outras unidades, desde que respeitados os seguintes critérios:

I – O diretório de rede deverá ter ciclo de vida definido, com data prevista para exclusão dos arquivos;

II – Caso os usuários envolvidos no projeto ou na atividade já possuam diretório de rede em comum, este deve ser utilizado, a não ser que não haja espaço suficiente para os arquivos;

III – A data de exclusão do diretório de rede poderá ser alterada, desde que precedida de alteração no cronograma do projeto, devidamente demonstrada no ato da solicitação.

Art. 45. A rede possuirá um diretório temporário – denominado "H:" – com acesso permitido a todos os usuários, destinado à transferência de documentos.

Parágrafo único. O conteúdo deste diretório não terá cópia de segurança e será excluído diariamente.

Art. 46. A SETIN, em conjunto com o gestor da unidade usuária do diretório de rede, será responsável pelo controle e pelo monitoramento das capacidades dos referidos diretórios da rede de computadores do Tribunal e dos tipos de arquivos que poderão ser armazenados em tais áreas.

Art. 47. A SETIN encaminhará ao gestor da unidade, quando solicitado, relatório gerencial contendo as seguintes informações:

I – Crescimento da área de armazenamento ocupada pela unidade nos últimos 30 dias; mais antigos.

II – Lista dos maiores arquivos armazenados pela unidade, bem como dos arquivos Art. 48. A capacidade de armazenamento dos diretórios de rede das unidades será fixa, mas poderá ser incrementada quando solicitado pelo responsável da unidade, desde que respeitados os seguintes requisitos:

I – Revisão do diretório pelos usuários para identificar arquivos que não são mais necessários, tais como: a. arquivos pessoais de usuários que não estão mais lotados na unidade; b. material para estudo ou aulas que não estejam relacionadas com as atividades desempenhadas no Tribunal; c. arquivos pessoais não associados ao trabalho; d. registros de eventos não relacionados à atividade da unidade.

II – O aumento da capacidade do diretório de rede não ultrapasse o limite de crescimento de 20% (vinte por cento) no período de um ano;

III – Aumentos superiores ao limite de 20% (vinte por cento) no período de um ano deverão ser precedidos de justificativa que demonstre mudanças no processo de trabalho que demande maior consumo de espaço.

Parágrafo único. Norma interna da SETIN, disponível na intranet do Tribunal, regulamentará o limite de tamanho dos diretórios, que será fixado pelo Comitê Gestor de TI – CGTI, subsidiado por estudo técnico apresentado pela SETIN.

Art. 49. Será vedada a cópia, em diretório da rede de computadores do Tribunal, dos seguintes tipos de arquivos:

I – imagens, músicas e filmes de qualquer formato;

II – programas não homologados ou não licenciados;

III – programas de conteúdo prejudicial à segurança do ambiente computacional;

IV – outros arquivos digitais cuja utilização não seja de interesse do Tribunal.

§ 1º A SETIN poderá excluir dos diretórios da rede os arquivos que se enquadrem nos incisos I a IV deste artigo, com prévio aviso, quando possível, e sem realizar cópia de segurança dos arquivos excluídos.

§ 2º Será autorizado o armazenamento de arquivos elencados no inciso I, desde que expressamente justificado.

Art. 50. Será responsabilidade do usuário da rede de computadores do TST:

I – utilizar os diretórios da rede somente para arquivar documentos referentes às suas atribuições funcionais;

II – primar pela eficiência e racionalidade na utilização dos recursos tecnológicos disponíveis, eliminando periodicamente os arquivos que não sejam necessários ou não façam parte do acervo de sua unidade.

Art. 51. O acesso efetuado pela rede de computadores do Tribunal será monitorado e registrado pela SETIN, podendo a qualquer momento ser efetuada auditoria, conforme estabelecido no Capítulo XIV deste Ato.

CAPÍTULO IX
DA UTILIZAÇÃO DE PROGRAMAS E APLICATIVOS

Art. 52. A instalação e a utilização de programas de computador no Tribunal estão sujeitas aos seguintes requisitos:

I – existência de licenças de uso em quantidade suficiente;
II – homologação pelos técnicos da CSUP;
III – conformidade com a atividade da instituição e com a área de atuação;
IV – compatibilidade com os demais programas utilizados;
V – adequação aos recursos computacionais disponíveis;
VI – obediência a planejamentos, cronogramas e prioridades existentes;
VII – análise pelos técnicos de Segurança da Informação.

Parágrafo único. Os programas instalados que porventura não atendam aos requisitos deste artigo poderão ser removidos pela CSUP, sem prévio aviso ao usuário e sem a realização de cópia de segurança.

Art. 53. A instalação de programas e aplicativos homologados, incluindo programas básicos, em equipamento de informática do Tribunal deverá ser executada, exclusivamente, por técnicos ou métodos autorizados pela SETIN.

Art. 54. É vedada a instalação de programa de terceiros, sem licença de uso regularmente contratada.

Art. 55. Caberá à CSUP manter o registro das licenças de uso de programas de terceiros utilizados pelo Tribunal.

Art. 56. A SETIN poderá autorizar a cessão de cópia de programa de computador adquirido ou contratado pelo Tribunal, em ambiente externo, nos termos da licença de uso.

Art. 57. A SETIN poderá realizar, para teste e avaliação, a instalação de programa ou aplicativo, com autorização do produtor, distribuidor ou revendedor, quando couber, pelo prazo estipulado na autorização.

Art. 58. É vedada a instalação e a utilização de programas e aplicativos de computador não homologados ou que descaracterizem os propósitos do Tribunal ou que possam oferecer riscos à segurança dos ativos de informação ou danificar o ambiente tecnológico do Tribunal.

Art. 59. A solicitação de instalação de programas e aplicativos homologados deverá ser encaminhada à SETIN pela Central de Serviços de TI.

Art. 60. A CSUP manterá publicada na intranet a listagem dos programas e dos aplicativos homologados para a utilização no Tribunal.

Art. 61. A CSUP deverá inventariar, sistematicamente e de forma remota, os programas e aplicativos instalados no ambiente tecnológico do Tribunal, sem prévia autorização do usuário.

Art. 62. A atualização dos programas e aplicativos instalados no âmbito do Tribunal poderá ser realizada pela equipe técnica da CSUP remotamente, sem prévia autorização do usuário.

Art. 63. O usuário será responsabilizado pela instalação ou pela execução não autorizada de programa não homologado pela SETIN, considerando-se a possibilidade de dano às instalações de informática do Tribunal.

CAPÍTULO X
DA UTILIZAÇÃO DE EQUIPAMENTOS DE TECNOLOGIA DA INFORMAÇÃO

Art. 64. Os dispositivos portáteis pertencentes ao parque computacional do Tribunal deverão possuir a mesma proteção das estações de trabalho.

Art. 65. É vedada a conexão direta de equipamento ou dispositivo portátil particular na rede cabeada de computadores do TST, sem a prévia verificação e autorização da equipe técnica da SETIN.

Parágrafo único. A não observância do disposto neste artigo implicará a responsabilização do usuário que efetuar a conexão.

Art. 66. Os dispositivos portáteis de armazenamento deverão ser verificados pelo programa de detecção e proteção contra vírus e outros programas maliciosos ao serem conectados à rede cabeada ou a equipamento pertencente ao Tribunal.

Parágrafo único. A não observância do disposto neste artigo implicará a responsabilização do usuário que efetuar a conexão.

Art. 67. A solicitação de verificação de equipamento ou dispositivo portátil para autorização de conexão na rede cabeada de computadores do Tribunal deverá ser encaminhada à SETIN pela Central de Serviços de TI, acompanhada de justificativa.

Art. 68. O acesso efetuado pelos dispositivos móveis no ambiente tecnológico do Tribunal será monitorado e registrado pela SETIN, podendo a qualquer momento ser efetuada auditoria, conforme previsto no Capítulo XIV deste Ato.

CAPÍTULO XI
DA UTILIZAÇÃO DE SERVIÇOS EM NUVEM

Art. 69. A utilização de serviços em nuvem, hospedados fora do ambiente computacional do TST, deverá observar:

I – a realização de análise prévia, visando assegurar as garantias fundamentais no tratamento das informações pessoais, segundo preconizam os incisos e os parágrafos do artigo 31 da Lei 12.527, de 18 de novembro de 2011 – Lei de Acesso à Informação;

II – a prévia classificação da informação hospedada pelo seu gestor quanto ao sigilo de seu conteúdo;

III – a definição de critérios de continuidade aceitáveis;

IV – a definição de critérios para garantir os princípios de confidencialidade, integridade e disponibilidade;

V – a definição de critérios para permitir a comunicação tempestiva e o adequado tratamento de incidentes de segurança computacional;

VI – a definição de critérios adequados à realização de auditorias de segurança da informação;

VII – definição do uso aceitável de dados, metadados, informações e conhecimentos tratados, inclusive sobre a vedação ao provedor ou a terceiros de utilização diversa da prevista em contrato;

VIII – definição de critérios de eliminação ou destruição definitiva de dados, metadados, informações e conhecimento, especialmente em momentos de transição contratual;

IX – requisitos necessários, para os casos de cancelamento, descontinuidade, portabilidade e renovação do referido instrumento contratual ou similar, bem como substituição de ambiente, que visem à eliminação e/ou à destruição definitiva de dados, metadados, informações e conhecimento;

CAPÍTULO XII
DA POLÍTICA DE MANUTENÇÃO, REMANEJAMENTO, DOAÇÃO OU DESCARTE DE EQUIPAMENTOS DE TI

Art. 70. Em caso de manutenção de equipamentos de TI, a unidade responsável da SETIN deverá considerar as seguintes recomendações:

I – equipamentos, informações ou softwares não devem ser retirados do local sem autorização prévia;

II – realizar backup e eliminar as informações do equipamento quando a manutenção for realizada por equipe externa ao Tribunal;

III – após a manutenção por equipe externa, inspecionar o equipamento para garantir que não foi alterado indevidamente e que não há mau funcionamento.

Art. 71. Em caso de remanejamento de equipamentos de TI, a unidade responsável deverá considerar a formatação do equipamento antes de realizar o seu remanejamento para outra unidade.

Art. 72. Em caso de doação ou descarte de equipamentos de TI, a unidade responsável da SETIN deverá formatar previamente o equipamento.

CAPÍTULO XIII
DAS BOAS PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO

Art. 73. Durante a execução das suas atividades profissionais, todos os usuários do TST, seja presencialmente, seja em teletrabalho, devem observar as seguintes recomendações:

I – guardar em local seguro informações sensíveis ou críticas que estejam armazenadas em papel, mídia eletrônica ou outro meio, especialmente quando o local de trabalho estiver desocupado;

II – desligar ou hibernar os computadores ao final do expediente;

III – bloquear os computadores com senha no caso de ausências curtas, por exemplo, para almoço, lanche e reuniões;

IV – utilizar somente equipamentos do próprio TST na realização do trabalho presencial.

CAPÍTULO XIV
DO CONTROLE, MONITORAMENTO E AUDITORIA DE RECURSOS TECNOLÓGICOS

Art. 74. A utilização de recursos tecnológicos, bem como o acesso aos ativos de informação no Tribunal serão registrados e monitorados pela SETIN, com o intuito de detectar e evidenciar incidentes de segurança.

Parágrafo único. Não será realizado o monitoramento de serviço de telefonia móvel ou fixa.

Art. 75. A SETIN é responsável por realizar auditorias ordinárias e extraordinárias nos ativos de Tecnologia da Informação do Tribunal.

§ 1° Auditorias ordinárias serão realizadas periodicamente, com o objetivo de avaliar a conformidade técnica de serviços, ferramentas e equipamentos em funcionamento no Tribunal.

§ 2° Auditorias extraordinárias serão requeridas por superior para apurar eventos que coloquem em risco a segurança dos ativos de informação e as boas práticas de utilização do ambiente tecnológico do Tribunal.

Art. 76. Estarão sujeitos à auditoria extraordinária os seguintes eventos de segurança:

I – Na estação de trabalho: alteração de arquivos e da configuração da estação de trabalho, instalação de programas de computador;

II – Nos dispositivos móveis: alteração de arquivos e da configuração do dispositivo, acessos ou manipulação de dados indevidos;

III – Nos sistemas informatizados e nos bancos de dados do Tribunal: acessos ou manipulação de dados indevidos;

IV – No correio eletrônico corporativo: envio e recebimento de mensagens eletrônicas indevidas;

V – No acesso à intranet, à internet ou a outro meio de acesso externo à rede de computadores do Tribunal: acessos e manipulação de dados indevidos;

VI – Na rede de computadores do Tribunal: alteração de arquivos e da configuração dos servidores.

Art. 77. A solicitação de auditoria em incidente não previsto neste Ato será analisada e deliberada pelo Comitê Gestor de Segurança da Informação.

CAPÍTULO XV
DA GESTÃO DE RISCOS, DE CONTINUIDADE E DE VULNERABILIDADES DO AMBIENTE TECNOLÓGICO

Art. 78. À SETIN caberá, periodicamente, a realização da gestão de riscos dos ativos de informação de TI.

Art. 79. Será mantido pela SETIN o processo de gestão de continuidade dos serviços críticos de tecnologia da informação, assim classificados pelo Comitê Gestor de TI ou pelos Comitês de Sistemas.

Art. 80. À SETIN caberá, periodicamente, a realização da gestão de vulnerabilidades dos ativos de informação de TI.

Art. 81. A CSUP manterá, instalado e atualizado, programa de detecção e proteção contra programas maliciosos e demais agentes nocivos à segurança dos ativos de informação no ambiente tecnológico do Tribunal.

CAPÍTULO XVI
DAS DISPOSIÇÕES GERAIS E TRANSITÓRIAS

Art. 82. Os responsáveis pela elaboração de termo de referência ou de projeto básico para aquisições ou contratações deverão incluir requisitos de segurança da informação de acordo com o objeto a ser licitado.

Art. 83. Os responsáveis pela elaboração de termo de referência ou de projeto básico para aquisições ou para contratações deverão incluir acordos de confidencialidade, conforme o objeto a ser licitado.

Art. 84. Caberá à SGSI e ao Comitê Gestor de Segurança da Informação a revisão periódica desta Política de Segurança da Informação.

Art. 85. A SGSI poderá, constatado o não cumprimento deste Ato, a qualquer momento, suspender o acesso concedido ao usuário.

Art. 86. A inobservância das disposições deste Ato implicará responsabilidade administrativa na forma da lei.

Art. 87. A SETIN terá prazo de 12 (doze) meses após a publicação desta Política de Segurança da Informação para eventuais adequações dos normativos aos requisitos deste Ato.

Art. 88. O presente Ato entra em vigor na data de sua publicação e revoga o Ato GDGSET.GP nº 764/2012.

(*) Republicado por força do Art. 2º do ATO TST.GP Nº 437, de 10/11/2020.

Fonte: Boletim Interno [do] Tribunal Superior do Trabalho, Brasília, DF, n. 45, p. 9-22, 13 nov. 2020. Republicação 1.